

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

**DONNA CURLING, ET AL.,
Plaintiffs,**

v.

**BRAD RAFFENSPERGER, ET AL.,
Defendants.**

Civil Action No. 1:17-CV-2989-AT

**DECLARATION OF J. ALEX HALDERMAN
IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION**

J. ALEX HALDERMAN declares, under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct:

1. My name is J. Alex Halderman. I am a Professor of Computer Science and Engineering and the Director of the Center for Computer Security and Society at the University of Michigan in Ann Arbor, Michigan. I submit this Declaration in support of Plaintiffs', Donna Curling, Donna Price, and Jeffrey Schoenberg (the "Curling Plaintiffs"), motion for Preliminary Injunction. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

2. I have a Ph.D., a Master's Degree, and a Bachelor's Degree in Computer Science, all from Princeton University.

3. My research focuses on computer security and privacy, with an emphasis on problems that broadly impact society and public policy. Among my areas of research are software security, network security, and election cybersecurity.

4. I have authored more than 85 articles and books. My work has been cited in more than 8,000 scholarly publications. I have served on the program committees for 31 research conferences and workshops, and I co-chaired the USENIX Election Technology Workshop, which focuses on electronic voting security. I received the John Gideon Award for Election Integrity from the Election Verification Network, the Andrew Carnegie Fellowship, the Alfred P. Sloan Foundation Research Fellowship, the IRTF Applied Networking Research Prize, and the University of Michigan College of Engineering 1938 E Award for teaching and scholarship.

5. I have published peer-reviewed research analyzing the security of electronic voting systems used in numerous U.S. states as well as in other countries. I have also investigated methods for improving the security of electronic voting, such as efficient techniques for testing whether electronic vote totals match paper vote records.

6. I have testified before the U.S. Senate Select Committee on Intelligence and before the U.S. House Appropriations Subcommittee on Financial

Service and General Government on the subject of cybersecurity and U.S. elections.

7. I have performed extensive hands-on security testing of the AccuVote TS and TSX electronic voting machines, which I understand are the two models of electronic voting machines used in Georgia. I published a peer-reviewed security evaluation of the AccuVote TS¹, and I performed a source code review of the AccuVote TSX as part of a study commissioned by the Secretary of State of California.² These studies discovered dozens of serious security vulnerabilities in the AccuVote hardware and software.

8. On August 7, 2018, I submitted a declaration in support of the Curling Plaintiffs' motion for a Preliminary Injunction.³ All of the conclusions and observations set forth in my initial submission remain true today; none of the events that have occurred in the intervening months have caused me to alter those conclusions.

9. Rather, new information has further confirmed the vulnerability of Georgia's election system, including proven risks posed by state actors as well as

¹ Ariel J. Feldman, J. Alex Halderman & Edward W. Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine*, Princeton University (2006), http://usenix.org/events/evt07/tech/full_papers/feldman/feldman.pdf.

² Joseph A. Calandrino et al., *Source Code Review of the Diebold Voting System*, University of California, Berkeley (2007), <http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/diebold-source-public-jul29.pdf>.

³ Dkt. No. 260-2.

unexplained risks posed by unidentified actors. For example, in his March 2019 Report, Special Counsel Robert Mueller concluded principally that “[t]he Russian government interfered in the 2016 presidential election in sweeping and systematic fashion.”⁴ The Special Counsel’s report further explained that foreign actors “sought access to state and local computer networks by exploiting known software vulnerabilities on websites of state and local governmental entities.”⁵ The Special Counsel also found that these foreign agents were successful in attacking at least one state and that their activities involved “more than two dozen states.”⁶ As noted prior to the Special Counsel’s final report, Georgia was targeted.⁷

10. In addition, Georgia experienced serious irregularities in its Lieutenant Governor’s race where there were significant “undervotes.” This suggests the potential for widespread malfunctions among the DREs, as well as potential malfeasance.⁸ Finally, in November 2018, former Georgia Secretary of

⁴ Robert S. Mueller, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election (Volume I of II)*, United States Department of Justice (March 2019), p. 1, <https://www.justice.gov/storage/report.pdf>.

⁵ *Id.* at 50.

⁶ *Id.* at 50.

⁷ See *United States v. Netyksho et al.*, No. 1:18-cr-00215-ABJ, Indictment ¶ 72, Dkt. No. 1 (D.D.C. July 13, 2018).

⁸ Kim Zetter, *Georgia voting irregularities raise more troubling questions about the state’s elections*, Politico (February 12, 2019), <https://www.politico.com/story/2019/02/12/georgia-voting-states-elections-1162134>.

State Kemp publicly acknowledged that there had been another intrusion into the State's voter registration system, prompting the FBI to investigate.⁹

11. As I noted previously, the only practical way to safeguard Georgia's upcoming elections is to discontinue the use of Georgia's DREs, require the use of optical scan paper ballots throughout Georgia, and mandate auditing of the results to ensure that the optical scanners are not attacked with malware to infect the automated counting of the ballots.


12. In addition, it is my understanding that Georgia intends to use Ballot-Marking Devices (BMDs) as a replacement for its DRE system. While I reserve judgment for a more extensive review of the equipment Georgia eventually chooses, BMDs will not remedy the existing vulnerabilities inherent to DREs and would continue to pose unacceptable risks to Georgia's election security. BMDs are touchscreen computers that create a computer-marked printout that is then tallied by an optical scanner. These machines—BMDs and optical scanners—are similarly susceptible to hacking and interference as Georgia's current electronic system. Programming errors or malicious attacks can cause BMDs to print selections

⁹ Alan Judd, *How Brian Kemp turned warning of election system vulnerability against Democrats*, Atlanta Journal Constitution (December 14, 2018), <https://www.ajc.com/news/state--regional-govt--politics/how-brian-kemp-turned-warning-election-system-vulnerability-against-democrats/iLOkpHK3ea39t8Eh4PCGxM/>.

different from the voter's intent, and there is no evidence that voters would reliably detect such errors in BMD printouts.

13. Furthermore, in typical BMD designs, the printouts from the BMD are tallied by reading a bar code, not by reading human-verifiable notations of their intended votes. As such, no voter would be able to verify that the bar code matches their selections. Malicious code that infected the BMDs could change the selections encoded in the bar code, and thereby change the vote recorded by the optical scanners without being detected. The proposed BMD system is merely a different electronic configuration posing the same inherent defects that Georgia's current system faces. Finally, as BMDs are a new and untested technology, there could be many more vulnerabilities associated with these devices that further examination and study would reveal.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 27th day of May, 2019 in Ann Arbor, Michigan.



J. ALEX HALDERMAN